

ブラック・マーケットには、わずか1万円ですぐに入手できる個人情報入りデータ(100MB)が登場 次々と巧妙になる、データ窃盗犯の手口

G DATA Software株式会社（代表取締役社長：Jag 山本、本社：東京都千代田区）は、インターネットを使ったデータ窃盗についての近況をレポートします。

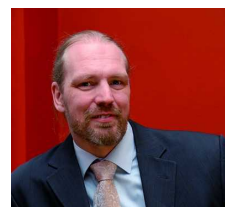
近年、サイバー犯罪者によるデータの窃盗、販売、不正使用による被害額は、年間で1500億円程度（約10億ユーロ）にもなっています。その収入源は、オンライン上で使用されているIDやパスワード、銀行口座番号、クレジットカード番号などであり、それらを盗み出すうえで、さまざまな策略が練られています。

一般的によく知られているような、ECサイトやカード会社、銀行などの偽ページに誘導するようなフィッシング・メールは、すでに古典的な手法となりました。また、ジューデータ・ウイルスラボ所長であるラルフ・ベンツミュラーによれば、2005年頃に流行したファームウェアとクライムウェアは、彼ら犯罪者のもっとも成功した事例となっており、今もよく使用されるものです。しかしさらに、ジューデータの研究によると、現在、新たな犯罪手法が登場しつつあります。この「新スタイルのデータ窃盗」のトリックと戦術について注意を促すことを、本レポートの目的とします。

個人情報の窃盗と販売は、今や、サイバー犯罪における最も効率の高いビジネスモデルとなっています。彼らは、以前は、オンラインバンキングのデータ窃盗を中心に活動していましたが、そのような活動の制限は、かなり以前にやめており、長い準備期間を経て、新たな窃盗手法をとるようになってきました。

「これだけ世界各国で個人情報の流出が話題となっているにもかかわらず、多くの個人ユーザーは自分の個人情報の価値を過小評価しています。犯罪者は、不正使用するか、もしくは現金に変えることを明確な目的として、そういったデータを収集しているということにもっと注意を向けるべきでしょう。

窃盗犯が他の人間にデータを売る場合の取引価格は、品質によってさまざまです。個人情報を含んでいるもののソートされていない状態のデータならば、驚くほど安価で、たとえば数100MBの容量のデータは1万円程度（約60ユーロ）でブラック・マーケットにて取引されています。このなかには、電子メールのアカウント、ネットの決済サービスの入力データ、オンラインバンキング情報などが含まれているのです。」（ラルフ・ベンツミュラー、ジューデータ・ウイルスラボ所長）



過去に何度か、データ窃盗の手口は大きく変わってきていますが、かつてならば、本物に見せかけたページに被害者を誘い込むような、フィッシング・メールがよく使われました。「ドメインに正しく入ったとしても、それが本当に正しいサイトであるとはかぎりません。DNSサーバに侵入することによって、また、PCを感染させ特殊なマルウェアを操ることによって、ニセモノのページに被害者をおびき寄せるのです。専門家さえ、なかなかそれらと本物を見分けられないでしょう。そのようなサイトで入力されたデータは、仕掛けた人間に自動的に送り届けられるのです」と、ベンツミュラーは述べています。

クライムウェア 犯罪者のもっとも効果的な武器

しかし、フィッシング・メールに対する保護システムの多様化やマスクミによる啓発運動などにより、随分とその手口が知られるようになり、仕掛け人たちは、新しい戦術に切り替えてきています。

今、フィッシング攻撃にもっともよく使用されているのは、トロイの木馬です。特に注目されているのは、「使い捨て型」のトロイの木馬です。たとえば、一度だけ使用され、個人情報などのデータの抜き出しに成功したあと、自然消滅するようなプログラムが組み込まれているものです。



「バンコス」(Bancos)の亜種や「ニューレッチ」(Neurech)のような巧妙なマルウェアは、ウェブサイトの内容を書き換えることができます。犯罪者が作った入力フォームを組み込んだり、場合によっては、ページまるごと書き換えてしまいます。そして、書き込まれたデータは、本物のサイトのサーバに送られると同時に、サイバー犯罪者の手にもわたるような仕組みになっています。それゆえ表面上は、まったく何事も起こらなかったかのようにことは進みます。口座からの不明な出金を確認されたときにはじめて、何が起こったのかに気づくのです。

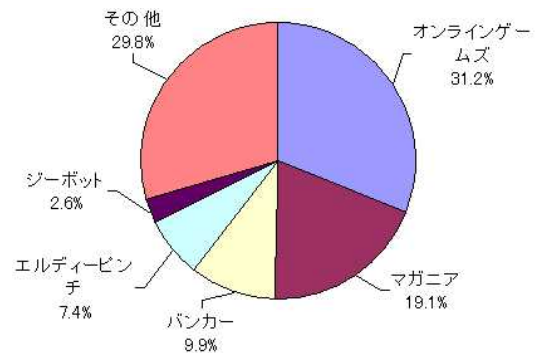
啓発と保護

アンチウイルス、アンチフィッシング、ファイアウォール、スパム対策などを結合した効果的なセキュリティソリューションの採用は、PC(インターネット)を使う以上は、今や必須のことではないでしょうか。しかし2008年2月にジーデータラボでの調査結果においては、ほぼ約半数の人たちがプロテクトなしにインターネットを利用していることが判明しました。このような現実、データ窃盗を試みる犯罪者にとって、格好の餌食となります。

データ保護の問題を真剣に受け止め、サイバー犯罪者たちの攻撃手法についての知識をもつことによって、彼らが遂行しようとする悪事からみを守るべきではないでしょうか。

【参考資料】「クライムウェア」トップ5

個人情報盗み取ろうとするマルウェアは、毎日のように、手を変え品を変え登場しています。そのなかでも、もっともよく登場している「クライムウェア」は以下のとおりです(右グラフも参照してください)。



ウイルス種名	割合	機能
オンラインゲームズ (OnLineGames)	31.2%	オンライン・ゲームのパスワードを見つけ出し犯罪者に送付。
マガニア (Magania)	19.1%	台湾のメーカー、ガマニアのオンライン・ゲームのログイン・データを盗む。
バンカー (Banker)	9.9%	オンラインバンキング・ページが呼び出されると、フォームに入力された全てのデータを盗む。
エルディーピンチ (Ldpinch)	7.4%	ブラウザ、電子メール・クライアント、インスタントメッセージャー、FTP プログラムとダイヤラーなどの設定におけるパスワードを見つけ出し、盗む。また、バックドアや他のマルウェアをインストールする。
ジーボット (Zbot)	2.6%	オンラインバンキングに使われる入力フォームや保護されたストレージ領域(たとえば、複数のパスワードが格納されたところ)から個人情報を盗む。

ジーデータソフトウェア エージー(G DATA Software AG)について

G DATA Software は、1985年に創業したドイツのセキュリティソフト会社です。EUを中心に、コンシューマーならびに法人向け製品を展開しています。日本法人は2007年に設立、主要製品は「アンチウイルス」「インターネットセキュリティ」「トータルケア」です。最大の特徴は、ダブルエンジンによる世界最高位のウイルス検出率であり、各誌・各テストで実証済みです。また、**フィッシング詐欺対策**、未知ウイルスへの防御、迷惑メールへの外国語フィルターなど、インターネットやメール環境を安全・快適にする機能を豊富に搭載しています。

*本ニュースリリースについて

本ニュースリリースに記載されている内容および製品情報については、市場動向、社会状況、経営方針の変更等により将来的に変更される可能性があります。本ニュースリリースに記載されている記載内容に関する永続的な整合性をG DATA Software株式会社が保証するものではありません。本リリースに記載されている各種名称、会社名、商品名などは各社の商標または登録商標です。

【本リリースに関する問合せ先】

G DATA Software 株式会社 101-0047 東京都千代田区内神田 2-8-1 富高ビル 3F 広報窓口：瀧本往人
E-mail: gdata_japan_info@gdatasoftware.com TEL: 03-3526-6605 URL: <http://www.gdata.co.jp/>